

## CHAPTER 6

### SECURITY OF COMMUNICATIONS SYSTEMS

#### A. GENERAL

1. This Chapter describes concepts for **physical** security of **communications facilities** located on and off **military** installations, to include mobile systems. **Specific** security support for facilities that require special security measures shall be coordinated between the concerned Components.

2. Because of the difference in location, physical layout and equipment, security considerations must be thoroughly assessed for each communications system. The physical security program shall be tailored to that particular facility or system.

#### B. POLICY

1. It **is** DoD policy that the protection provided to DoD communication facilities and systems shall be sufficient to ensure continuity of operations of critical users and the facilities they support. These include nuclear weapon delivery units and storage facilities, main operating bases (for allied air forces), and primary command and control elements. The determinations on strategic importance, both to the United States and its allies, shall be based upon whether or not each mobile system or facility processes, transmits, or receives, telecommunications traffic considered crucial by the National Command Authorities (**NCA**), the Chairman, Joint Chiefs of Staff, or the Commanders in Chief of the Unified and Specified Commands.

2\* Communications systems **play** a major role in support of each DoD Component's mission, providing operational communications in both peacetime and wartime. These are attractive targets due to limited staffing, isolated location and mission. Therefore, security for these systems must be an important part of each command's physical security program.

3. The DoD Component must review the host installation's implementation of physical security measures during inspections oversight, and staff visits.

4. Access shall be controlled at all communications facilities; only authorized personnel shall be allowed to enter. Facilities should be designated and posted as Restricted Areas.

5. Depending on regional conditions, commanders should consider locating **enough** weapons and ammunition at communications facilities to arm designated onsite personnel. If arms are stored at the facilities, appropriate security measures and procedures shall be employed in accordance with DoD 5100.76-M (reference (h)).

**6. Existing** essential structures should be hardened against attacks. This **includes** large antenna support legs, antenna horns, operations building and cable trays. Future construction programs for communications facilities should include appropriate hardening of essential structures.

### **C. RESPONSIBILITIES**

1. DoD Components shall have each major command identify critical communications facilities and mobile systems.

2. DoD Components shall have each commander of a major command ensure that a security **plan** is developed for each communications facility and **mobile** system under his or her command. The plan shall include emergency security actions and procedures for **emergency** destruction of sensitive equipment and classified information. The plan may be an annex to an existing host installation security plan; only the applicable parts of the total plan shall be distributed to personnel at the facility or mobile system.

**3.** The owning DoD Component shall arrange for security of off-installation facilities and mobile systems with the closest U.S. military installation. This includes contingency plans for manpower and equipment resources during emergencies. These arrangements can be made by establishing a formal **agreement**, such as an interservice support agreement. Whether the facilities are located on or off the installation, or mobile, installation commanders are responsible for security of communications facilities for which they provide host support.

**4.** Operations, maintenance, and communications personnel at the **facility** or mobile system are the most important factor in security. DoD Components shall have each commander of a major command ensure implementation of a training program to ensure that **assigned** personnel understand their day-to-day security **responsibilities**, are familiar with the vulnerabilities of the facility, and are prepared to implement emergency security actions. The training program shall include the following:

**a.** Security procedures and personal protection skills for **assigned** personnel.

**b.** The use of weapons and communications equipment for protecting the facility or mobile system.

**c.** Awareness of local terrorist threats and other activity in the area.

5. DoD Components may issue additional instructions governing security of the communications facilities.

#### D. MOBILE COMMUNICATIONS SYSTEMS

**In** accordance with Chapter 2 of this Regulation, a security operational concept or standards shall be developed for mobile systems to describe the **minimum** level of" security for the system in the expected operational environment.